Advocates for Rural Broadband
Paul Kelly
President
Kelly Worthington
Executive Vice President

August 22, 2016

FILED VIA ECFS
Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

RE: Notice of Ex Parte Communication, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

On August 18, 2016, the undersigned, Derrick Owens and Gerry Duffy representing WTA – Advocates for Rural Broadband ("WTA") met with Daniel Kahn, Sherwin Siy, Brian Hurley, and Melissa Kirkel (via telephone), to discuss the Commission's proceeding to develop rules regarding broadband customer privacy and data security. WTA recommended modifications to the Commission's proposal to reduce burdens on small carriers to avoid diverting resources away from broadband infrastructure deployment.

WTA described the CPNI practices of its small rural local exchange carrier ("RLEC") members, which typically includes either refraining entirely from any use of CPNI for marketing purposes or alternatively providing customers the option to opt-out of marketing upon signing up for service, through biennial privacy notifications, and allowing customers to opt-out through customer service upon request. The most common example of use of CPNI by WTA members is the offering of increased broadband speed tier packages during inbound or outbound customer calls. Additionally, any sharing of information typically occurs solely between the RLEC and its affiliates that provide services to their customers or third-parties that provide services related to the provision of telecommunications services, including but not limited to billing, help-desk representatives, and installation contractors.[1] WTA urged that the Commission must continue to permit the sharing of information between RLECs, their affiliates, and vendors.

WTA noted that regardless of whether carriers rely on generalized marketing or use CPNI for marketing purposes, all small carriers will need to review and revise existing policies and procedures to reflect the Commission's proposed expanded view of the scope of section 222. For example, WTA expressed concern regarding the proposal to require affirmative opt-in consent from customers for carriers to use otherwise publicly available information such as name, telephone number, and address. Currently, "under section 222 and the Commission's rules, a carrier could contact all of its customers or all of its former customers, for marketing purposes, by using a customer list that contains each customer's name, address, and telephone number, *so long as it does not use CPNI to select a subset of customers from that list*."[2] WTA urged the Commission against

[1] WTA members that provide access to CPNI to third-party vendors obtain CPNI protection agreements requiring that vendors protect CPNI.

[2] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary*

adopting rules that prohibit carriers from contacting their own customers without targeting of individuals or a subset of customers, for example to obtain responses to customer satisfaction surveys, promote digital literacy events, announce annual meetings, or alert all current and former customers of new services being offered.

WTA also expressed concern regarding the impact of the proposed narrowed scope of "communications-related" services that could disrupt the ability for small carriers to continue offering bundles of products and services unless a customer (or prospective customer) opts-in. Were the Commission to narrow its definition of "communications-related" services as proposed, carriers would need to obtain opt-in consent for marketing of services that today require only an opportunity to opt-out. Most – if not all – voice providers also provide broadband service, and consumers increasingly expect their broadband provider to offer enhanced services such as technical/device support and managed Wi-Fi solutions that help consumers get maximize and manage their broadband connections. Therefore, the Commission should retain the ability for small carriers to use an opt-out mechanism for marketing the provision and maintenance of customer premises equipment and other information services consumers expect voice and broadband telecommunications carriers to offer.

In addition to retaining current definitions, the Commission should also permit small BIAS providers to grandfather existing opt-out approvals as it has done in the past.[3] Allowing small providers to grandfather existing opt-outs will substantially limit the impact of the proposed rules on small BIAS providers. It would also help avoid consumer confusion and frustration because small providers would not be required to seek and obtain approvals they have already obtained consistent with current voice CPNI rules and existing practices.

WTA urged the need for the Commission to scale its expectations to the different resources and operating environments of WTA members and other small providers in regards to the mechanism for customers to exercise their rights with respect to CPNI. The vast majority of small BIAS providers engage several third-party vendors for most—if not all—of their network operations and billing systems, including the provision of online customer accounts.[4] Vendors' existing systems are proprietary and are not intended to build automated reports tailored to each individual customer. Small providers will be reliant on disparate vendors to integrate billing, mapping, and other systems that contain incongruent datasets in various formats and in different locations (for example, secured in hard-copy in a locked file cabinet, housed in the cloud or on physical servers located on the carrier's premises). Small carriers simply do not have the size and scale to force their vendors (most of whom are larger in size) to integrate their systems for numerous small companies that each use a different combination of vendors and/or in-house expertise. Small providers will also be reliant on vendors for the development and licensing of a secure user interface (or modify existing online account systems) to allow customers to access their data.

WTA also explained that its members do not currently, and have no plans to, retain customer Internet browsing histories and related information on an individual subscriber basis because the cost of a change in security

---

Network Information and Other Customer Information, CC Docket No. 96-115, Order, 13 FCC Rcd 12390, 12395-97, ¶¶ 8-9 (1998). *See also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, CC Docket No. 96-115, et al., Order on Reconsideration and Petition for Forbearance, 14 FCC Rcd 14409, 14487-88, ¶¶ 146-47 (1999) (adopting the Common Carrier Bureau's reasoning and conclusion that to prohibit carriers from using their own customer lists without additional targeting would be anomalous to the intent of Section 222).

[3] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, CC Docket No. Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, ¶ 85 (2002) (allowing grandfathering of approvals).

[4] WTA also noted that some of its small BIAS provider members do not currently provide customers any online account access and would need to develop online access capabilities as a prerequisite to providing a "privacy dashboard."

posture and the necessary upgrades to storage and data processing capabilities would significantly outweigh any potential monetary benefit derived from data relating to the small subscriber bases of RLECs. Rather than mandating that carriers retain additional customer data and provide a "privacy dashboard," WTA urged the Commission continue to permit carriers to provide customers an opportunity to change their preference at any time through any combination of methods.[5] Exempting small BIAS providers from a privacy dashboard requirement would extend existing protections for consumer privacy while avoiding the diversion of resources away from broadband deployment or increased data security measures.[6]

With regard to the proposed data security rules, WTA stated that the Commission's rules must account for the unique circumstances, small sizes and limited resources of RLECs, their affiliates, and other small BIAS providers. Because risk management requires tough decisions regarding which risks are reasonably acceptable in light of an organization's activities, size and resources, WTA urged the Commission to provide flexibility for small carriers and refrain from imposing specific security requirements beyond a generalized duty to employ reasonable security measures. WTA also argued that size should be a factor for consideration when assessing the implementation of reasonable security measures in order to avoid unreasonably holding small carriers with only a handful or two of employees to the same standard as providers that employ armies of technical and security professionals and drive industry best-practices.[7] This is a key point because WTA noted that other respondents in the record,[8] the NIST Cybersecurity Framework,[9] the CSRIC Working Group 4 Report,[10] the Federal Trade Commission,[11] the Cox Breach Consent Decree[12] and pending legislation before Congress all encourage or include explicit references to size as a factor in determining the appropriateness of a data security and risk management strategy.

WTA elaborated on arguments raised in its initial and reply comments regarding specific components of the Commission's data security proposal that would unduly burdensome for small carriers. For example,

---

[5] *See* 47 C.F.R. § 64.2008(d)(3)(v).

[6] WTA is unaware of, and the record lacks reference to, any examples in which small carriers' customers were unable to modify their privacy preferences or otherwise access account information.

[7] WTA noted that although the proposed rules include an assessment of the nature and scope of a BIAS provider's activities, the proposed rule and NPRM are ambiguous regarding whether the Commission "nature and scope" includes consideration of size and available resources.

[8] *See* Comments of American Cable Association at 44; Comments of Rural Wireless Association at 10; Comments of Wireless Internet Service Provider Association at 31-32; Reply Comments of U.S. Small Business Administration at 3-4.

[9] *See* NIST, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, (rel. Feb. 12, 2014) available at http://www.nist.gov/cyberframework/upload/cybersecurityframework-021214-final.pdf.

[10] Communications Security Reliability and Interoperability Council IV, "Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report," at 35 (rel. March 2015) *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (including a section specifically tailored to small carriers and noting that small and mid-sized carriers "have unique circumstances and challenges that may influence their approach to implementing the Framework and providing macro-level assurances").

[11] FTC, "Data Security," *available at* https://www.ftc.gov/datasecurity (*last accessed* Aug. 22, 2016) (stating that "a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities").

[12] *Cox Communications, Inc.*, Order and Consent Decree, 30 FCC Rcd 12302 (Enf. Bur. 2015) (requiring implementation of "[a]dministrative, technical, and physical safeguards that are reasonable in light of Cox's size and complexity, the nature and scope of Cox's activities, the sensitivity of the PI/CPNI collected or maintained . . . and the risks identified through risk assessments").

mandating that small carriers conduct a minimum number of risk assessments or penetration tests each year would require small carriers to hire outside vendors at a substantial expense.[13] Similarly, requiring that all customer data be encrypted when stored would also pose significant cost and implementation challenges for small carriers in light of their limited resources and reliance on outside vendors for billing and other network solutions. Likewise, mandating that senior managers overseeing information security possess certain credentials or qualifications is untenable for small staff organizations where each employee juggles multiple hats and small companies would either need to invest in certifications for existing employees or hire new employees that already have the necessary certifications at a higher salary. Such a requirement would raise costs for carriers without any demonstrable benefit, particularly when most small providers already rely on third-party vendors for technical assistance with security and RLECs need to dedicate every available dollar to meeting broadband deployment obligations.

WTA also noted the substantial challenge for small BIAS provides to train and monitor the data security practices of their vendors. As previously discussed, the vast majority of small BIAS providers rely on third-parties for security services, including employee training for CPNI and data security. Whereas WTA's members may be able to obtain general contractual commitments to comply with CPNI rules and data security requirements, WTA's members have little to no visibility into the internal practices of their vendors nor do they enjoy leverage to engage in ongoing oversight. Accordingly, the Commission cannot reasonably hold small providers responsible for training their vendors' employees or continually monitoring the CPNI and data security practices of their vendors.

Finally, WTA noted that small carriers require sufficient time after the discovery of an apparent breach for investigation and resolution prior to notifying affected customers. Ten days may be a worthy goal, but requiring small providers dependent on third-parties to investigate whether a breach actually occurred, identify affected customers, and issue notifications within 10 days will likely result in carriers providing inaccurate or incomplete information, leading to a combination of over-notification and distrust. WTA supports flexibility in this regard by requiring customer notification as soon as reasonably practicable.

Pursuant to Section 1.1206 of the Commission's rules, a copy of this letter is being filed via ECFS.

Sincerely,
/s/ *Patricia Cave*
Patricia Cave
Director, Government Affairs

Cc (via email): Daniel Kahn
Sherwin Siy
Brian Hurley
Melissa Kirkel

[13] Costs for engaging third-party vendors to conduct penetration testing varies widely based on the size and complexity of the networks and systems involved. WTA estimates an average cost of $5-7,000 per test, an overwhelming cost for carriers with only a few hundred or thousand potential customers over which to spread their costs.